



PATENT  
Docket No. INTEL/17852

**IN THE UNITED STATES PATENT  
AND TRADEMARK OFFICE**

Applicants: Zimmer, et al.	)	I hereby certify that this paper is
Serial No.: 10/719,428	)	being deposited with the United
Filed: November 21, 2003	)	States Postal Service with
Assignee: Intel Corporation	)	sufficient postage as first class
For: "Methods and Apparatus to Provide	)	mail in an envelope addressed to:
Protection for Firmware Resources"	)	Commissioner for Patents, P.O.
Group Art Unit: 2131	)	Box 1450, Alexandria, VA 22313-
Examiner: Unknown	)	1450 on this date:
	)	<u>4/2/2004</u>
	)	<b>Date</b>
	)	<u>Mark C. Zimmerman</u>
	)	Mark C. Zimmerman
	)	Registration No. 44,006
	)	Attorney for Applicant(s)

**INFORMATION DISCLOSURE STATEMENT**

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

The patents and/or publications listed on the enclosed PTO Form-1449 are submitted pursuant to 37 CFR §§ 1.56, 1.97, and 1.98. Copies of the patents or publications are enclosed.

## METHOD OF PAYMENT

- ☒ No fee is required.
- ☐ Attached is a check in the amount of \$


The Commissioner is authorized to charge any fee deficiency required by this paper, or credit any overpayment, to Deposit Account No. 50-2455. A copy of this paper is enclosed.

Correspondence Address:

Respectfully submitted,

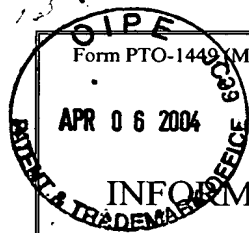
GROSSMAN & FLIGHT, LLC.  
20 N. Wacker Drive  
Suite 4220  
Chicago, Illinois 60606  
(312) 580-1020

By:

  
Mark C. Zimmerman  
Registration No.: 44,006

Attorneys for Intel Corporation

4/2/2004  
Date



Form PTO-1449 (Modified)

U.S. Department of Commerce  
Patent and Trademark Office

Atty. Docket No.

INTEL/17852

Serial No.

10/719,428

Applicant

ZIMMER, et al.

Filing Date

11/21/03

Group Art Unit

2131

## INFORMATION DISCLOSURE STATEMENT

(Use several sheets if necessary)

## U.S. PATENT DOCUMENTS

*EXAMINER INITIALS	DOCUMENT NUMBER	ISSUE DATE	INVENTOR(S)	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE

## FOREIGN PATENT DOCUMENTS

*Examiner Initials	Document Number	Publication Date	Country	Class	Subclass	Translation Yes No	

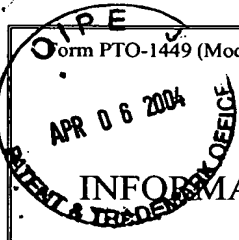
## OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, etc.)

	Compaq Computer Corporation, Intel Corporation, Microsoft Corporation, Phoenix Technologies LTD., Toshiba Corporation. <i>Advanced Configuration and Power Interface Specification</i> . Compaq Computer Corporation, Intel Corporation, Microsoft Corporation, Phoenix Technologies LTD., Toshiba Corporation, August 25, 2003. pp. All. Pages of particular interest: 13-15, 17, 37, 88-89, 99, 113-115.
	Intel Corporation. <i>An Overview of the Trusted Platform Module (TPM) and the Trusted Computing Group's (TCG) Trusted Platform Architecture</i> . Trusted Computing Group, Inc., May 5, 2003. pp. 1-6.
	<i>TCG PC Specific Implementation Specification</i> . Compaq Computer Corporation, Hewlett-Packard Company, IBM Corporation, Intel Corporation, Microsoft Corporation, September 9, 2001. pp. 1-71. Pages of particular interest: 25-27, 33, 34, 39.
	Trusted Computing Group. <i>Introduction and Brief Technical Overview</i> . Trusted Computing Group, August 1, 2003. Slides 1-25.
	Windows Platform Design Notes. <i>Security Model for the Next-Generation Secure Computing Base</i> . Microsoft Corporation, 2003. pp. 1-13.
	Windows Platform Design Notes. <i>NGSCB: Trusted Computing Base and Software Authentication</i> . Microsoft Corporation, 2003. pp. 1-16.
	Windows Platform Design Notes. <i>Hardware Platform for the Next-Generation Secure Computing Base</i> . Microsoft Corporation, 2003. pp. 1-10
	Microsoft Corporation. <i>The Next-Generation Secure Computing Base</i> . Microsoft Corporation, April 2003. pp. 1-2.

EXAMINER

DATE CONSIDERED

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

	U.S. Department of Commerce Patent and Trademark Office	Atty. Docket No. <b>INTEL/17852</b>	Serial No. <b>10/719,428</b>
		Applicant <b>ZIMMER, et al.</b>	
		Filing Date <b>11/21/03</b>	Group Art Unit <b>Unknown</b>

# INFORMATION DISCLOSURE STATEMENT

(Use several sheets if necessary)

	Grawrock, D. <i>LaGrand Architecture SCMS – 18</i> . September 2003. Slides 1-57.
	<i>TCPA Technical Overview for EFI</i> . January 17, 2002. Slides 1-77.
	Ferron-Jones, M; Girard, L. <i>LaGrande Technology &amp; Safer Computing Overview</i> . Intel. Slides 1-19.
	Intel Corporation. <i>LaGrande Technology Architectural Overview</i> . Intel Corporation, September 2003. p. 1-8.
	Windows Platform Design Notes. <i>Secure User Authentication for the Next-Generation Secure Computing Base</i> . Microsoft Corporation, 2003. pp. 1-11.
	Kozierok, C. M. Power Management, [online], [retrieved on 10/20/2003]. Retrieved from the Internet <URL <a href="http://www.pcguide.com/ref/cpu/char/powerPM-c.html">http://www.pcguide.com/ref/cpu/char/powerPM-c.html</a> >.
	Grawrock, D. <i>Trusted Computing Platform Alliance</i> . Intel Corporation. Slides 1-24.
	Intel Corporation. AGP V3.0 Interface Specification. Intel Corporation, September 2002. pp. 1-143. Pages of particular interest: pp. 122-123.
	Trusted Computing Group, Incorporated. <i>Main Specification Version 1.1a</i> . Trusted Computing Group, Incorporated, 2003. pp. All. Pages of particular interest: 2-6, 8-13, 14-15, 83-91, 97, 305, 306.
	Intel Corporation. <i>Extensible Firmware Interface Specification</i> . Intel Corporation, 2002. pp. All.

EXAMINER	DATE CONSIDERED
<p>*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance <u>and</u> not considered. Include copy of this form with next communication to applicant.</p>	